

VPN을 적용한 인터넷 전화 단말기의 성능평가에 관한 연구

정회원 이 성 기*, 유 승 선**, 이 명 재***, 곽 훈 성*

Study on Evaluation of Performancen on Internet Phone(VoIP) using the VPN

Seong gi Lee*, Seung Sun Yoo**, Myeong jea Lee***, Hoon-Sung Kwak* *Regular Members*

요 약

암호화된 인터넷 전화 단말기의 통화품질 측정을 하기위해 실험환경을 구성하여 캡슐화에 따른 지연을 실험한 결과 구현 인터넷 전화기와 일반 VoIP 전화기와의 지연시간의 차이는 최대 5ms 이하였다. 이러한 지연시간의 대부분은 VPN의 터널링을 위한 패킷 캡슐화에 소요되는 지연시간으로 예상할 수 있다 따라서 일반 VoIP 전화기와 본 연구에서 제시한 VPN을 적용한 VoIP 전화기와의 통화품질의 차이는 무시할 만하였다 또한 하나의 패킷 당 프레임 개수를 다르게 하여 통신하는 동안 네트워크 전체 패킷의 크기를 구하여PAC과 PNS사이의 캡슐화 과정이 네트워크 부하에 가장 많은 영향을 주는 요소로 작용한다 따라서 본 연구에서는 최적의 패킷 당 프레임 수를 산출하기 위해 패킷에 할당 하는 프레임 개수를 증가시켜 통화 품질에 문제가 없는 중 단간 지연을150ms 이내로 할 때 패킷 당 프레임 개수는 2~3개가 적합하다는 결론을 얻었다

Key Words : VoIP, VPN, PNS, PAC, end-to-end delay

ABSTRACT

To measure the performance of call quality, we have built the experiment environment and observed that the delay caused by encapsulation between internet and VoIP telephones is under 5ms at most. The major delay is assumed to be the time required to capsulate the packet for tunnelling of VPN. Because the difference of average delay time is under 4ms~5ms, the difference of call quality between VoIP and VoIP telephone adopting VPN is negligible. We have concluded that the capsulation process between PAC and PNS is the major factor influencing the network load by changing the number of frames in a packet during communication Also, we have concluded that the most suitable frame numbers is tow or three by adding the frame numbers in a packet to obtain the suitable frames in a packet and setting up end-to-end delay under 150ms.

I. 서 론

인터넷 전화(VoIP)는 음성의 전달을 기존의 전화망(PSTN)이 아닌 IP(Inter protocol)네트워크를 통하여 전달하는 새로운 개념의 통신 수단이라 할 수

있다. 또한 인터넷 전화는 음성뿐만 아니라 인터넷으로 부가되는 모든 서비스를 전화기를 통하여 지금보다 아주 저렴하게 제공 받을 수 있다는 장점이 있으며, 광대역 액세스 망들이 인터넷에 접속되고 이 틀 위에서 VoIP(Voice of IP)나 P2P(Peer to Peer)

* 전북대학교 대학원 컴퓨터공학과 박사수료(www2www@empal.com), ** 비맥(주) 기술이사(yss1962@paran.com),
*** ICC(주) 대표이사(lmj@iccmate.com), * 전북대학교 컴퓨터공학과 교수(hskwak@moak.chonbuk.ac.kr)
논문번호 : KICS2005-03-105, 접수일자 : 2005년 3월 14일

등의 다양한 새로운 통신 응용서비스들이 제공됨에 따라 인터넷 문화는 새로운 통신 수단으로 우리 생활에 다가 올 것이다. 그러나 인터넷을 이용한 전화(Voip)는 인터넷의 특성상 하나의 망에서 다수의 일반 대중이 동시에 사용하는 통신 수단이므로 도청과 같은 음성 보안등이 사회 문제로 나타날 수 있다. 그러나 현재 인터넷 전화에서 효과적인 보안 기능을 적용하는 연구가 이루어지고 있지 못하고 있다. 이것은 VoIP 프로토콜의 복잡성과 네트워크 장비 연동의 문제점 등으로, VoIP 시스템에서 보안기능을 제공하는 것은 실제로 대단히 어려운 일이다 따라서 도청과 같은 보안 문제를 해결하기 위한 다양한 제안들이 표준화 단계에서 논의되고 있으나 실제 구현 할 수 있는 상세 규정이 나오기까지 상당히 시일이 걸릴 것으로 예상된다. 따라서, 본 논문에서는 참조문헌[9]과 같이 인터넷 전화기에 사용자 인증과 데이터 보안을 효과적으로 수행하기 위하여 VPN을 이용한 음성 보안 인터넷 전화를 개발하였으며 본 연구에서는 개발된 음성 보안 인터넷 전화기의 성능에 관하여 실험을 통해서 측정 평가 하였다

II. 음성 보안 인터넷 전화기 통화 절차

본 연구에서 개발한, 음성 보안 인터넷 전화기는 SIP(Session Initiation Protocol) 프로토콜 스택을 적용하였으며, 인터넷 전화 단말기에 도청방지를 위하여 PPTP(Point-to-Point Tunneling Protocol)를 적용하여 PAC(PPTP Access Concentrator) 기능을 구현하였다[참조문헌 9 참조]. 그리고 구현 단말기와 기존 VoIP 전화기의 중단 간 지연시간을 측정하여 음성품질의 성능을 분석하고 보안기능이 적용된 인터넷 전화기의 타당성을 입증하였다. 그리고 통화연결에는 SIP를 사용하였고, 개발된 PAC는 PPTP Client side 부분을 담당하며 PNS(PPTP Network Server)와 하나의 제어 연결을 생성한다 제어 연결은 PPTP 터널링을 하기 전에 PPTP 연결을 제어하기 위해 설정하는 절차이다 제어 연결을 생성하기 위해서는 먼저 PAC에서 PNS로 제어 연결을 요청하고 PNS로부터 응답을 수신 한 후 외부로 보내는 호(Call)에 대한 설정을 요청한다. PNS로부터 호 설정에 대한 응답을 수신 한 후 마지막으로 PAC와 PNS가 서로 연결된 Link의 정보를 설정하기 위해서 Set-Link- Info 메시지를 사용하여 제어 연결 설정을 완료한다. 제어 연결 설정이 완료가 되면 PAC와 PNS사이에 PPP(Point-to-Point Protocol)를 이용

하여 링크 Configuration을 협상하고 지원할 프로토콜들이 무엇인가를 협상하게 된다 먼저 LCP (Link Control Protocol)를 이용하여 PPP Link를 설정하고, 인증 프로토콜을 사용할 것인가 아닌가, 만약 사용한다면 어떤 알고리즘을 사용할 것인가를 협상한다. 또한 압축알고리즘을 사용할 것인가 아닌가를 협상한다. LCP과정을 통해서 협상된 Option들을 가지고 다음에 적용할 프로토콜이 결정된다 본 연구에서는 인증프로토콜을 사용하는 것으로 협상을 하였고 CHAP(Challenge Handshake Authentication Protocol)을 사용하기로 했기 때문에 PNS에서 PAC에게 CHAP Challenge 메시지를 보내서 인증을 요청한다. 그러면 PAC에서는 PNS로부터 얻은 데이터와 자신의 user-id와 password를 결합하여 CHAP response를 생성하여 응답한다. 그러면 PNS는 수신한 데이터 값이 올바르면 CHAP success 메시지로 응답하여 인증절차를 마치게 된다. 또한 LCP의 과정 중에서 압축알고리즘을 사용하겠다고 협상을 하였기 때문에 다음 절차는 압축알고리즘으로 어떤 프로토콜을 사용할 것인가를 협상하게 된다 그러면 동시에 지원할 Network layer의 프로토콜을 협상하게 된다. 본 연구에서, 압축 알고리즘으로는 PPP 패킷의 압축 알고리즘을 협상하는데 사용되는 MPPC(Microsoft Point-To-Point Compression)을 사용하였으며, Stateless Mode를 선택하고, 128bit encryption을 이용 하였다. Stateless Mode를 선택하게 되면 PPP 패킷의 암호화를 위한 프로토콜인 MPPE(Microsoft Point-To-Point Encryption) 패킷 format의 Coherency Count값이 모든 패킷 마다 변하게 설정하여 이전 패킷과 별개로 사용되도록 하는 것이다. 네트워크계층은 IP(Internet Protocol)를 사용하기로 하여 IPCP(Internet Protocol Control Protocol)가 네트워크 관련 정보를 PNS로부터 얻어 오게 된다. PAC의 사설 IP 주소와 사설 망, 사설 게이트웨이 IP 주소등과 같은 정보를 얻어서 PAC의 네트워크 계층을 설정한다

위의 모든 과정이 끝나면 초기 준비 단계는 완료가 되어 모든 장치들이 하나의 VPN으로 연결되는 것이다. 이로써 각 PAC에서 프록시 서버로 접근할 수 있고 이미 각 PAC에는 프록시 서버의 사설 IP가 설정되어 있어서 사설망으로 연결된 뒤에는 프록시 서버에게 자신의 private ip를 이미 할당된 VoIP 전화번호와 함께 등록한다. 등록절차가 완료되고 통화하고자 하는 전화번호로 전화를 걸면 SIP 프로토콜 절차에 따라서 전화 통화가 가능하게 된다

III. VPN 시그널링 프로토콜

네트워크를 운영하다 보면 내부 통신뿐만이 아닌 외부로부터의 접근 필요성을 느끼게 된다. 어디서든 IP 네트워크에 접속만 할 수 있으면 IP 주소로 직접 리소스를 가져갈 수 있다. 하지만 그것은 보안에 심각한 취약적인 문제가 있다. 가상 사설망(VPN : Virtual Private Network)은 인터넷과 같은 공유 또는 공용 네트워크를 통한 연결을 포함하는 사설 네트워크의 확장으로 통신망 기반시설을 터널링 프로토콜과 보안 절차 등을 사용하여 개별기업의 목적에 맞게 구성된 데이터 네트워크이다. 지점간 링크를 에뮬레이션 하기 위해 데이터는 공유 또는 공용 인터넷네트워크를 통과하여 목적지에 도달할 수 있도록 라우팅 정보를 제공하는 머리글에 의해 캡슐화된다. 개인 링크를 에뮬레이션 하기 위해 전송되는 데이터는 암호화 되어 기밀성이 유지된다. 공유 또는 공용 네트워크에서 차단되는 패킷은 암호 키가 없으면 암호화될 수 없는데, 개인 데이터가 캡슐화되고 암호화되는 링크를 가상 사설 네트워크(VPN) 연결이라고 한다. VPN 연결은 사용자가 인터넷과 같은 공용 인터넷네트워크에서 제공하는 하위 구조를 사용하여 가정에서나 이동 중에도 회사 서버에 원격 액세스 연결을 할 수 있게 해 준다. 사용자의 입장에서 볼 때 VPN은 컴퓨터, VPN 클라이언트, 회사 서버인 VPN 서버 간의 지점 간 연결이다. VPN 연결은 또한 회사가 인터넷과 같은 공용 인터넷네트워크를 통해 지리적으로 떨어져 있는 사무실이나 다른 회사와 보안이 유지되는 통신을 유지하면서 연결을 라우팅할 수 있게 해 준다. 인터넷에서 라우팅 된 VPN 연결은 논리적으로 전용 WAN 링크 역할을 한다. 원격 액세스 연결 및 라우팅 된 연결과 함께 VPN 연결을 통해 기업은 시외 전화나 구내전화 전용 회선 또는 인터넷 서비스 제공자(ISP) 전용 회선을 사용할 수 있다. PPTP를 사용하는 VPN 연결은 다음과 같은 속성을 갖는다.

- ① 캡슐화
- ② 인증
- ③ 데이터 암호화
- ④ 주소 및 이름 서버 할당

IV. 구현 VoIP 단말기의 통화 품질 성능 평가

소리 품질과 대화 품질은 네트워크의 성능 및 네

트워크 장비 운용의 기술적인 면에서 영향을 받으므로 통화품질은 소리와 대화 품질의 질적인 평가에 의해 정의될 수 있다. 다음 세 가지는 통화 품질에 영향을 주는 요소이다.

4.1 명확성(Clarify)

통화 품질 측정에서 음질의 명확성은 음성 시그널의 충실성(Fidelity), 명확(Clearness), 소리 왜곡(Distortion)의 해소 정도, 인지 가능성(Intelligibility)에 대해 나타낼 수 있다.

4.1.1 UDP 패킷 손실률(%)

음질의 명확성에 영향을 주는 요소들 중의 하나가 패킷 손실인데 VoIP 네트워크에서 UDP 같은 비 연결형 전송 프로토콜을 사용함으로 음성 패킷 손실이 발생하게 된다. 이러한 음성패킷손실은 음성 정보의 상실을 의미하므로 통화품질에 영향을 준다. UDP 패킷 손실률이 클수록 상대방의 목소리가 끊기는 등의 통화품질 저하가 발생 할 수 있다.

4.1.2 음성 코덱(Voice Codec)

음성 코덱 역시 음질의 명확성에 영향을 주며 아날로그 음성을 디지털 형태의 비트 스트림으로 변환시키며 압축기술을 사용하여 전송에 필요한 대역폭을 줄이기 위해 불필요한 정보를 제거 한다. 본 연구에서 사용한 G.723.1 코덱은 낮은 비트속도로 멀티미디어 서비스의 음성이나 다른 오디오 신호 요소들을 압축하는데 사용할 수 있는 압축기법을 규정하는 것으로, 코더에는 5.3Kbps와 6.3Kbps의 두 가지 비트속도가 관련되어 있는데 6.3Kbps의 비트속도는 MP-MLP기술에 기초한 것으로 품질이 더 뛰어나다.

4.2 종단간 지연(End-to-End Delay)

VoIP 네트워크 종단간의 지연은 음성 신호를 송신자에서 수신자까지 전달하는 전송지연이며 값이 클수록 통화 시 거리감이 느껴질 수 있고 IP 네트워크 지연과 VoIP 장비지연으로 나눌 수 있다. IP 네트워크 지연은 전달지연(propagation delay)과 처리지연(handling delay)로 구분할 수 있는데 전달지연은 광섬유나 구리를 사용하는 네트워크에서 광속에 의해 발생하는 지연이고, 처리 지연은 직렬화(serialization delay)지연으로 음성경로를 따라 음성 정보를 처리하는 장치들에 의해 발생한다. 또한 처리 지연은 패킷 처리지연(Packet Processing Delay), 패킷 스위칭라우팅 지연(Packet Switching/Routing

delay) 및 IP 네트워크 내 패킷들의 불규칙한 도착 현상 및 제한된 전송로의 속도 때문에 패킷 스위치 라우터의 입력과 출력 포트에서 지연이 발생하는 대기열 지연(Queuing Delay)이 있다. 라우터의 대기열 지연은 VoIP 네트워크에서 종 단간 지연에 가장 영향을 주는 것으로 이러한 네트워크 내의 변화되는 지연들 때문에 패킷의 도착 시간의 불규칙한 현상이 발생하게 된다 VoIP 장비 지연은 VoIP 게이트웨이와 단말기 사이 전송로의 수신부와 송신부에서 음성시그널 처리 때문에 발생하고 상당한 지연을 초래한다. 이 처리지연은 인코딩과 디코딩의 코덱 지연시간이 포함되어 있고 코덱 종류에 따라 음성 시그널을 압축하는데 소요되는 추가적인 지연이 발생 한다. VoIP 장비의 송신부에서는 패킷화 지연이 발생하는데 음성정보를 패킷 내에 넣는데 소요되는 시간을 말하며 패킷 크기가 크면 더 많은 시간이 소요된다. 그러나 작은 패킷은 패킷화 지연을 축소시키지만 불필요한 헤더의 증가로 네트워크 대역폭의 효율을 감소시킨다 그림 1은 통화품질을 측정하기위한 종단간의 처리지연을 나타낸 것이다 종단간 지연되는 요소는 Client에서 음성 패킷을 전송하기위한 지연 장비 및 네트워크를 접근하기 위한 지연, IP 패킷의 큐잉을 하기 위한 지연, 패킷화 및 에코를 제거하기위한 게이트웨이 지연 PSTN망으로의 접근을 위한 지연 등으로 구분 될 수 있다 특히 본 연구에서 개발된 VPN 기반 VoIP 단말기는 그림 1의 Client지연 부분에서 PAC과 PNS 사이의 캡슐화 과정이 포함되어 터널링을 통한 음성 패킷을 전달하기 때문에 일반 VoIP 전화기에 비교하여 캡슐화 지연이 추가 된다. 그 외의 종단간 지연은 일반 VoIP 전화기와 같게 된다.

또한 에코(Echo)는 송신자의 음성이 송신자의 귀에 되돌아오는 소리로 통화 품질은 소리품질과 대화품질의 질적인 평가에 의해서 정의될 수 있는데 VoIP 네트워크에서는 그림2와 같이 위에서 언급한 3가지 요소 즉, 명확성, 종 단간 지연, 에코에 영향을 받고 그 요소들 간에는 복잡한 관계를 가지고 있다. 따라서 "Voice Quality Space"가 작아질수록 통화품질이 향상됨을 알 수 있다

본 연구에서는 3가지 요소 중 기존의 VoIP 전화기와의 차이점인 캡슐화 과정이 추가 되어서 발생하는 지연을 중점적으로 실험하고자 한다 즉 명확성과 에코는 VPN을 적용한 VoIP 전화기와 기존의 VoIP 전화기와 큰 차이가 없다고 판단되므로 시험 파라미터에서는 제외한다 VoIP 전화기의 통화 품

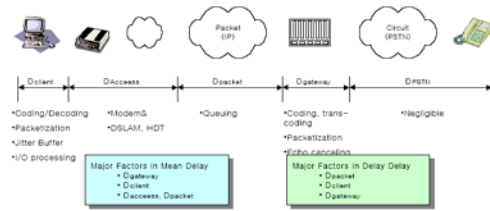


그림 1. VoIP 종단간 지연 요소



그림 2. 음성 명확성, 지연 및 에코의 관계

질을 예측하기 위한 방법으로 E-model은 ITU-T G.107에 제시된 실험모델로 여러 가지 전송 파라미터들을 기본으로 하여 0에서 100까지의 값을 가지는 R-scale로 품질을 측정한다[3]. 대략 70 이상이면, 청각적으로 무리가 없는 양호한 통화품질 수준이고 이 R값을 이용하여 MOS를 추정한다. MOS (Mean Option Score)는 음성 코덱의 성능을 수량화할 수 있는 일반적인 벤치마크 이다 통화품질과 사운드는 일반적으로 청취자에 따라 기준이 주관적이기 때문에 광범위한 청취자와 샘플 재료를 바탕으로 하는 것이 중요하다 MOS 측정은 각 음성 샘플에 대해 1(나쁨)에서 5(우수함)까지의 등급을 평가하는 청취자 그룹을 대상으로 시행하며 그 점수의 평균을 구하여 MOS 점수를 구한다. 0~5까지의 범위의 수치로 사람이 느끼는 평균적이고 주관적인 음성 품질지수 이다. 대략 3.6 이상이면 사람의 청각이 느끼기에 별 무리가 없는 Fair(양호)한 품질이라고 할 수 있다. R 값에 영향을 주는 파라미터들과의 관계는 다음과 같다

$$R = R_0 - I_s - I_d - I_e + A$$

- R_0 : 기본적인 신호 대 잡음(Signal-to-Noise)
- I_s : 음성신호와 동시에 전송되는 감쇠요인
- I_d : 지연 감쇠(Daley Impairment)
- I_e : 저 대역폭 코덱 감쇠
- A : 보상 값

표 1. 통화 품질에 대한 범주 정의

Range of R	Speed Quality category	User Satisfaction
90 ≤ R < 100	Best	very satisfied
80 ≤ R < 90	High	satisfied
70 ≤ R < 80	Medium	Some users dissatisfied
60 ≤ R < 70	Low	Many users dissatisfied
50 ≤ R < 60	Poor	Nearly all users dissatisfied
R < 50		Not recommended

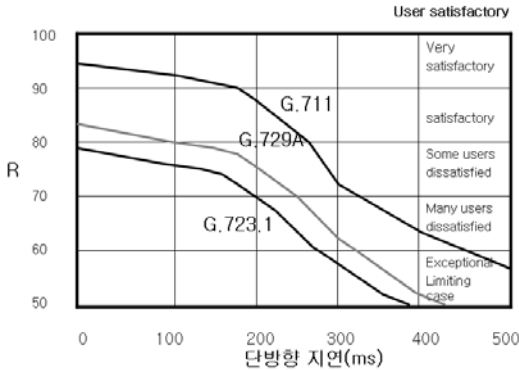


그림 3. VoIP 코덱 비교

다음 표 1은 ITU-T Recommendation G.109에 정의되어 있는 R-scale에 따른 사용자의 만족도를 나타낸다[1]. R 값이 50 미만인 것은 수용할 수 없는 통화 품질을 의미한다.

그림 3은 가장 많이 사용되는 VoIP 코덱 G.711, G.729A 및 G.723의 통화품질 R값을 비교하여 나타내고 있다. G.711과 비교하면 G.729A와 G.723.1 코덱들은 R 값이 크기 때문에 R 값에 대하여 수용될 수 있는 단 방향 지연폭이 매우 적어진다. G.723.1을 사용하는 경우 단 방향 지연이 짧아도 통화품질이 만족 상태(R ≥ 80)를 제공할 수 없음을 보여주고 단 방향 지연이 120ms~150ms 정도 되어야 사용자가 만족한 통화 품질을 인식 할 수 있다 [4]. 또한, G.729A의 경우 단 방향 지연이 100ms 이내이어야 만족상태를 제공할 수 있다

ITU-T G.114[5]에서 서술한 단 방향 지연은 3가지 요소(인코딩/디코딩/패킷화+지터 버퍼 지연, 전송 지연, 전달지연) 이고, TIA/EIA/TSB116[6]에서 통화품질에 영향을 주는 지연문제를 해결하는데 권고 사항은 다음과 같다

- 음성 프레임 크기와 패킷내의 음성 프레임 수를 줄인다.

- 지터버퍼 지연을 가능한 줄인다.
- 단방향 지연을 가능한 줄인다.
- 불규칙한 지연을 방지하기 위해서 음성 트래픽을 위한 PQ 스케줄링과 RTP 헤더압축, 데이터 패킷 Fragmentation 등의 방식을 사용한다.
- 저속 시리얼링크를 사용하지 않는다

VoIP 네트워크에서 종단간의 지연을 어떻게 처리하느냐가 성공적인 VoIP 서비스를 제공하는 중요한 부분이다. 이를 위해 목표 네트워크에 대한 지연을 초래하는 요소들을 대상으로 목표치를 예상하는 것이 중요하다. 본 연구에서 G.723.1 코덱을 사용한 경우, VoIP를 이용한 음성통화 시에 일반적인 지연을 계산하면 다음 표 2와 같이 예상할 수 있다. 표에서 보는 바와 같이 단방향의 전체 예상 지연시간은 161ms로 본 연구에서는 기존의 VoIP 전화기의 개발 지연시간의 성능평가 기준으로 한다. ITU-T G.114[5]에서 단 방향 지연이 150ms 이내이면 우수한 통화 품질로 규정하고 있으며 300ms 이상의 지연은 통화품질에 문제가 있는 것으로 규정하고 있다

표 2. 단방향의 전체 지연 예상 시간

지연요소	예상지연시간
네트워크 인터페이스(1.54Mbps)	1ms
프레이밍(G.723.1 코덱)	30ms
처리 시간(최악의 경우)	10ms
버퍼링(추가적인 버퍼링이 없을 경우)	0ms
패킷화(2프레임/패킷)	30ms
미디어 접근 지연	10ms
라우팅	50ms
지터 버퍼링(one buffer)	30ms
= 단방향의 전체 예상 지연 시간	= 161ms

V. 구현 VoIP 전화기 통화 품질 측정

구현 VoIP 단말기의 실험환경은 그림 4와 같이 구성하였다. 그리고 패킷의 도달 간격 시간과 네트워크상의 지연 및 부하를 시험 분석을 통하여 VPN 기반으로 한 보안기능을 적용한 SIP의 가능성을 보이고자 한다

실험망은 그림 4에서와 같이 3개의 PAC과 각 로컬네트워크에 프록시 서버 PNS를 라우터로 연결하여 구성하였다. 여기에는 10개의 서브네트워크가 있으며, PNS는 PPTP Server side 부분을 담당하는 곳으로 PAC로부터 Control-Connection 설정 요청이

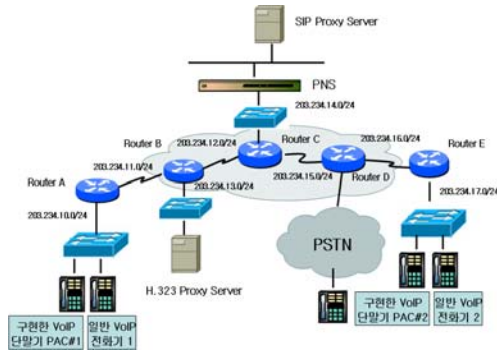


그림 4. VPN 기반의 SIP 실험 환경

오면 그에 대한 응답을 하여 PAC와의 사이에서 터널을 생성한다. 이미 생성된 터널을 통하여 PAC와 PPP를 이용하여 VPN을 형성한다.

PAC은 PPTP Client side 부분을 담당하는 곳으로 PNS와 터널을 생성하여 사설 망의 일원으로 참여 한다. 프록시 서버는 SIP 프로토콜을 이용하여 VoIP전화 통화를 위해서 필요한 Server로서 현재 SIP UA들의 정보를 가지고 있다 PNS는 PPTP Server Side가 구현되어 있는 장비로 PAC#1과 PAC#2의 user-id와 password 정보를 가지고 있으며 VPN을 구성하기 위한 private ip pool을 가진다. 또한 2개의 네트워크 인터페이스가 있는데 로컬네트워크 인터페이스는 사설망 구성을 연결하고 외부네트워크 인터페이스는 인터넷망을 연결 한다 또한 1개의 PPTP 인터페이스를 가지고 있고 외부네트워크 인터페이스를 통해서 수신되는 GRE 패킷을 암호화하여 라우팅 테이블에 의해서 로컬망이나 또 다른 사설망의 client에게 전달한다.

PAC#1와 PAC#2는 PPTP Client Side가 구현되어 있는 VoIP 단말기로PNS의 public ip와 port번호를 이미 알고 있다 PNS에게 인증을 받기 위한 자신의 user-id와 password를 가지고 있다. 초기화 및 전화 통화 과정은 다음과 같다

- ① PAC#1이 PNS에게 tunnel을 생성하기 위해서 PPTP 제어 연결 생성 절차와 같이 control-connection 메시지를 전송하여 PNS로부터 응답을 받는다.
- ② PAC#1이 생성된 tunnel을 통해서 PPP를 구동하여 인증절차를 마치고 private ip를 얻는다.
- ③ PAC#1이 수신된 private ip를 이용하여 내부에 pptp0라는 가상 내부 인터페이스를 생성한다
- ④ PAC#1이 SIP의 registration 기능을 통하여

PNS 뒤에 있는 Proxy Server에게 자신의 SIP 관련 정보를 등록한다. 이제부터는 VoIP 전화 통화가 가능한 상태가 된다.

- ⑤ PAC#2도 위의 ①~④ 과정과 같이 진행되어 VoIP 전화 통화가 가능한 상태가 된다.
- ⑥ PAC#1에서 수화기를 들고 PAC#2의 전화번호(2134)를 눌러 전화를 건다.
- ⑦ PAC#1에서 SIP메시지를 터널을 통해서 프록시 서버에게로 전달한다 터널을 통해서 송신되는 모든 메시지는 암호화되어 전송된다
- ⑧ PNS에서 외부 인터페이스로 수신된 GRE header를 가지는 패킷을 decryption하여 내부에 있는 private ip header의 destination ip를 얻어 내어 자신의 local 네트워크의 단말기의 주소이면 로컬 인터페이스로 전달을 해주고 아니고 또 다른 외부 망에 있는 private 단말기의 주소이면 다시 터널을 통해서 암호화하고 외부 인터페이스로 전송하여 PAC#2에 도착하도록 한다. 본 시험에서는 통화 품질의 각 측정 요소 중 가장 큰 영향을 미치는 단 방향 전달 지연에 대해 RTT값을 측정하여 본 연구에서 구현 VoIP 단말기의 음성품질이 전달 지연 기준인 150ms에서 200ms 사이에 지연시간이 포함 되는 것을 보이고자 한다 그러나 암호를 해석해야 하는 PNS는 통화량이 많을 때 집중화 현상이 발생하므로 PNS의 성능은 고려를 하여야 한다

5.1 RTP 패킷포맷

RTP 패킷은 UDP 데이터그램의 페이로드로 전달되며, 매우 간단한 헤더 포맷을 사용하고 있는데 이는 애플리케이션 데이터에 많은 오버헤드가 더해지는 것을 방지하려는 것이다 보통 실시간 애플리케이션은 많은 대역폭을 필요로 하는데 지연을 줄이고 애플리케이션의 RTP 전송을 효율적으로 하기 위해 메시지크기를 줄이고 헤더를 작게 한다 SIP에서 사용되는 패킷은 G.723.1 코덱을 사용한 경우 전체 64바이트의 IP 패킷에서 IP헤더와 옵션을 제외하면 8 바이트의 UDP 헤더와 36 바이트의 RTP 패킷으로 구성된다. RTP패킷은 다시 12바이트의 헤더와 24바이트의 음성 데이터로 구분되고 64바이트는 이 실험에 쓰인 SIP 애플리케이션이 채택을 하고 있는 G.723.1(6.3K) 코덱이 사용하는 암호화 데이터의 전체 크기이다. 음성압축 코덱 종류에 따라 전송되는 음성 데이터의 길이는 다음과 같다

- G.723.1=>6.3Kbps, 30ms마다 24bytes씩 전송
- G.729A=>8Kbps, 10ms마다 10bytes씩 전송
- G.711=>64Kbps, 20ms마다 160bytes씩 전송

또한 IP 패킷에 캡슐화되는 데이터 길이는 다음과 같다.

- G.723.1의 경우(64bytes)
private-ip header(20) + UDP header(8) + RTP header(12) + voice data(24)
- G.729A의 경우(50bytes)
private-ip header(20) + UDP header(8) + RTP header(12) + voice data(10)
- G.711의 경우(200bytes)
private-ip header(20) + UDP header(8) + RTP header(12) + voice data(160)

5.2 캡슐화 지연

VPN의 PPTP 프로토콜을 사용하고 터널링을 구성하여 통화하는 경우는 그렇지 않은 경우와 비교하여 캡슐화 과정을 거치기 때문에 중단간의 지연 시간의 차이가 나타날 것이고 그 차이를 조사하고자 한다. 측정 PAC에서 음성패킷을 보내고 네트워크 모니터링 도구인 스니퍼(Sniffer)를 통하여 되돌아오는 시간(Round Trip Time)과 패킷 순서를 측정하여 지연을 측정하였다. 라우팅의 경로상의 차이에서 발생하는 지연을 배제하기위해 VPN을 쓰지 않는 경우에도 같은 경로를 거치도록 실험 환경을 구성하였다.

그림 4에서와 같이 구현한 VoIP 단말기 PAC #1과 PAC #2의 경로와 같이 일반 VoIP전화기 #1, 일반 VoIP 전화기 #2의 경로를 구성하였다. 따라서 VPN을 적용한 VoIP 전화기와 일반 VoIP 전화기의 차이는 터널링을 위한 캡슐화(Encapsulation and Decapsulation) 오버헤드만 남게 된다. 두 경우의 차이는 RTT 값을 구하면 알 수 있다. 본 실험을 통해 얻은 각 코덱별 RTT 값은 다음 표 3과 같다.

본 실험에서 1차적으로 네트워크의 부하가 없는 상태에서 음성데이터를 터널링을 통하여 암호화한 경우와 일반 인터넷 전화기의 RTT 값을 비교 하였다. 실험 결과 VPN을 적용한 VoIP 전화기의 RTT는 표 3에서 보는 것과 같이 데이터 길이에 따라 5ms~11ms였고 일반 VoIP 전화기의 RTT는 데이터 길이에 따라 1ms~3ms 였다. 즉, VPN을 적용한 인터넷 전화기와 일반 VoIP 전화기와의 지연시간의

표 3. encryption 대 no-encryption의 RTT 값 비교표

데이터 길이 (byte)	프레임수	no-encryption	encryption	Differences
64(G.723.1)	1	1ms	5ms	4ms
88(G.723.1)	2	1ms	5ms	4ms
112(G.723.1)	3	1ms	5ms	4ms
136(G.723.1)	4	2ms	6ms	4ms
160(G.723.1)	5	2ms	6ms	4ms
184(G.723.1)	6	2ms	6ms	4ms
208(G.723.1)	7	2ms	7ms	5ms
696(G.723.1)	8	2ms	8ms	6ms
1088(G.723.1)	9	3ms	11ms	8ms

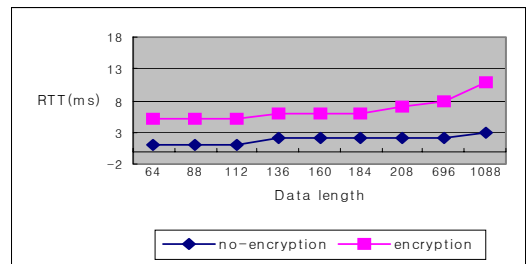


그림 5. G.732.1을 사용한 경우 RTT 값 비교

차이는 최대 8ms 이하이고, 대부분은 VPN의 터널링을 위한 패킷 캡슐화에 소요되는 시간으로 볼 수 있다. 그림 5에서 보는 바와 같이 종 단간 지연 실험결과를 종합해 보면 데이터의 길이가 클수록 지연시간의 차이는 증가하는 양상을 보였지만 데이터 길이가 1000byte를 넘는 경우는 없을 것이고 일반적으로 하나의 패킷에 1개의 프레임을 전송한다고 했을 때 지연시간의 차이를 보면 4ms 이하이고 최대 7개의 프레임을 한번에 전송한다고 했을 때에도 최대 데이터 길이는 208 byte를 넘지 않고 RTT의 차이는 5ms를 넘지 않았다. 표 2에서와 같이 본 연구에서 기준치로 잡았던 161ms(최악의 경우)에 캡슐화로 인한 지연시간을 합해도 165ms 정도이고, ITU-T의 권고안에서 정한 만족한 통화를 할 수 있는 단 방향 지연의 기준치인 150ms~200ms 안에 있으므로, 기존의 VoIP 일반 전화기와 본 연구에서 제시한 VPN을 적용한 VoIP와의 통화품질의 차이는 무시할 만하다

그림 6은 G.729A 코덱을 사용했을 경우 1개에서 최대 9개의 프레임을 1개의 패킷에 넣어 전송할 경우, 암호화한 경우와 그렇지 않은 경우의 전송지연 차이를 보인 것이다 위에서 언급했듯이 VPN을 적

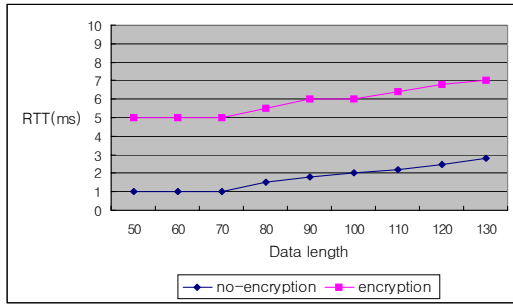


그림 6. G.729A를 사용한 경우 RTT 값 비교

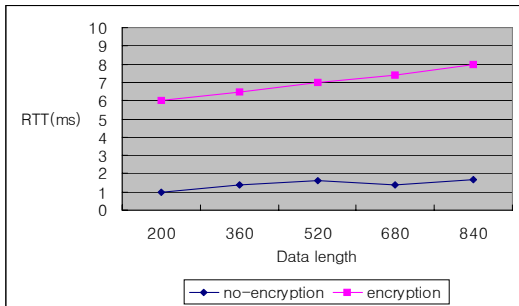


그림 7. G.711을 사용한 경우 RTT 값 비교

용한 VoIP 단말기와 일반 VoIP 단말기의 지연시간 차이는 최대 5ms를 넘지 않는다.

그림 7은 G.711 코덱을 사용했을 경우 1개에서 최대 5개의 프레임이 1개의 패킷에 넣어 전송할 경우 암호화한 경우와 그렇지 않은 경우의 전송지연 차이를 보인 것이다. VPN을 적용한 VoIP 단말기와 일반 VoIP 단말기의 지연시간 차이는 최대 6ms를 넘지 않는다.

5.3 네트워크 부하

VoIP의 SIP 프로토콜을 이용한 음성 통화 시에 네트워크상에 존재하는 부하에 초점을 두고 하나의 패킷 안에 몇 개 프레임을 전송하는 것이 적절한가를 측정하였다. 하나의 패킷에 한번에 많은 프레임을 보내어 대기시간이 길어지는 것과 프레임을 적게 보내어 빠른 대기시간을 기대하는 것에 대하여 논의할 여지가 있다. 본 연구에서 사용한 SIP 애플리케이션은 하나의 패킷 안에 64바이트의 프레임을 전송한다. 그림 8은 하나의 패킷 당 프레임 개수를 다르게 하여 통신하는 동안 구한 네트워크 전체 패킷의 크기에 대한 것인데 PAC과 PNS 사이에 캡슐화하인해 64 바이트 헤더가 더해지므로, VPN을 적용한 VoIP 단말기를 사용할 경우 하나의 패킷에 몇

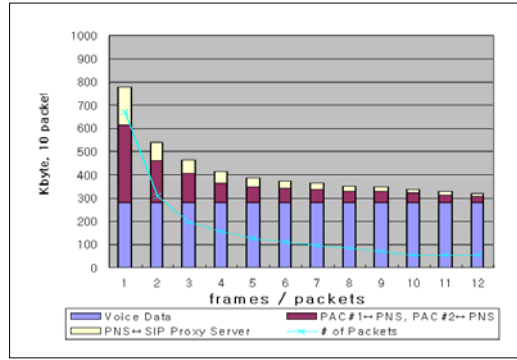


그림 8. 네트워크 부하

개의 프레임을 전송할 것인가가 매우 중요하다. VoIP 단말기 노드의 수를 증가 시킬수록 네트워크의 대역폭을 절약하는 것이 필요하다. 그러나 하나의 패킷에 무작정 많은 프레임을 실어 전송한다면 지연 시간이 커져 좋은 음성 품질의 서비스를 제공하기 어려울 것이다.

5.4 패킷당 프레임 수

가장 적합한 패킷당 프레임수를 얻기 위해 그림 9는 패킷 도달 간격을 도시한 그래프이다. 가운데 2선은 99% 신뢰를 갖는 구간을 이은 것 이고 바깥쪽 2선은 최고와 최악의 경우에 패킷 도달 간격을 그린 것이다. 종단 간 지연을 16 문제점을 없애기 위해 한 개의 패킷에 한 개 0ms~150ms로 할 때 패킷당 프레임 개수는 2~3개가 적합하다. 그러나 현재 구현 인터넷 전화기의 대부분은 초기지연으로 1개 프레임을 넣어 전송하는 추세이고 인터넷 전화기의 보급으로 음성 패킷 데이터가 많아질 경우에는 네트워크의 부하를 고려하여 한 개의 패킷에 2~3개의 패킷을 넣어 전송하는 것이 바람직 할 것이다.

특히, 한 개의 패킷에 여러 개의 음성 프레임을 전송할 경우 RTT 시간을 측정하여 보았듯이 코덱에 따라 지연시간의 차이가 났고 위에서 언급했듯이 암호화할 데이터의 길이가 G.723.1의 경우 한 개의 패킷에 한 개의 프레임으로 암호화할 데이터의 길이는 64bytes이며 30ms 마다 암호화하여 터널을 통해 전송하게 하고, 2개의 프레임일 경우 88bytes이며 60ms 마다 암호화하여 터널을 통해 전송하게 된다. 그리고 3개의 프레임일 경우 112bytes 이고 90ms 마다 암호화하여 터널을 통해 전송하게 된다. 그러나 G.729A일 경우 하나의 패킷에 1개의 프레임을 전송할 경우 50bytes이며 10ms 마다 암호화하여 터널을 통해 전송하게 되고, 2개의 프레임

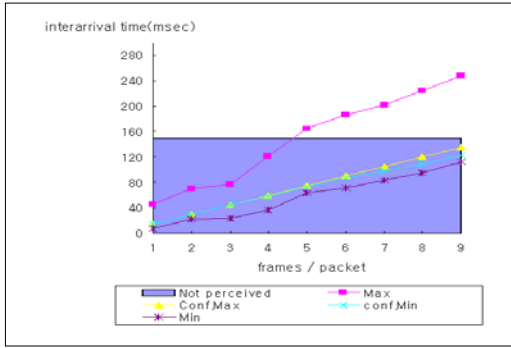


그림 9. 패킷 당 프레임 수 변화에 의한 패킷 도달 간격

일 경우 60bytes이고 20ms 마다 암호화하여 터널을 통해 전송하게 되고, 3개일 경우에는 70bytes이며 30ms마다 암호화하여 터널을 통해 전송하게 된다 즉, 암호화 할 데이터의 길이가 G.723.1일 경우 최대 112bytes이고, G.729A일 경우 70bytes 이라 하더라도 기존의 인터넷 전화기와 지연시간의 4ms 정도 발생하고 전체 150ms 이내의 지연 시간이 발생하여 코덱의 종류에 따라서는 음성 품질의 문제는 발생하지 않는다

VI. 결론

본 연구에서 개발한 도청방지용 인터넷전화기의 호 완료율 성능을 측정하기 위하여 Call length를 10초로 설정하였다 PAC 사이에서 tone을 보내고 확인하는데 걸리는 시간이 총 10초가 되지 않으면 다시 통화를 시도하여 Call length가 15초 정도 길어 질 수 있도록 하였다. 이러한 방법으로 24시간 호를 발생시켜 운용한 후 호 완료율이 100%인 것을 확인 하였다. 또한 통화품질 측정을 하기위해 실험환경을 구성하여 캡슐화에 따른 지연을 실험한 결과 구현 인터넷 전화기와 일반 VoIP 전화기와 지연시간의 차이는 최대 5ms 이하였다. 대부분은 VPN의 터널링을 위한 패킷 캡슐화에 소요되는 지연시간으로 예상할 수 있고 평균적으로 지연시간의 차이는 4ms~5ms 이하이므로, 일반 VoIP 전화기와 본 연구에서 제시한 VPN을 적용한 VoIP 전화기와 통화품질의 차이는 무시할 만하다

VoIP의 SIP 프로토콜을 이용한 음성 통화 시에 네트워크상에 존재하는 부하에 초점을 두고 하나의 패킷 안에 몇 개 프레임을 전송하는 것이 적절한가를 측정하였다 PAC과 PNS 사이에 캡슐화로 인해 64 바이트 헤더가 더해지므로 VPN을 적용한 VoIP

단말기를 사용할 경우 VoIP 단말기 노드의 수를 증가 시킬수록 네트워크의 대역폭을 절약하는 것이 필요하기 때문에 하나의 패킷에 몇 개의 프레임을 전송할 지는 중요하다 그러나 하나의 패킷에 무작정 많은 프레임을 실어 전송한다면 지연 시간이 커져 좋은 음성 품질의 서비스를 제공하기 어려울 것이다

본 연구에서 사용한 SIP 애플리케이션은 G.723.1 코덱을 사용할 경우 하나의 패킷 안에 24바이트의 음성 데이터를 전송 한다 하나의 패킷 당 프레임 개수를 다르게 하여 통신하는 동안 네트워크 전체 패킷의 크기를 구하여 PAC과 PNS사이의 캡슐화 과정이 네트워크 부하에 가장 많은 영향을 주는 요소로 판단되었고, 가장 적합한 패킷 당 프레임수를 얻기 위해 패킷당 프레임 개수를 증가시켜 다음 패킷 도달 간격을 구하여 종단 간 지연을 160ms~170ms로 할 때, 패킷당 프레임 개수는 2~3개가 적합하다는 결론을 얻었다 따라서 인터넷 전화기의 최대 단점으로 인식될 수 있는 도청을 방지하기 위하여 VPN(Virtual private network)기술을 인터넷 전화기에 접목하여 도청을 방지할 수 있는 토대를 마련하였다. 그러나 본 연구에서 사용된 PPTP 프로토콜은 제어연결(Control Connection)메시지가 암호화가 되지 않는다는 점과 인증기능이 없다는 단점으로 중간에서 제어연결메시지를 가로채서 분석할 수 있기 때문에 보다 완벽한 암호화(Security)가 이루어 질 수 없다는 문제점을 여전히 내포하고 있다 이 문제는 L2TP가 보완하고 있다 PPTP는 IP 기반 인터넷네트워크가 반드시 필요한 반면에 L2TP는 패킷 중심의 네트워크이면 어디서나 사용이 가능하다 좀 더 확장성이 있고 보안의 방식을 IPSec을 채택했다는 점이다 주로 인증서 기반의 IPSec을 사용하여 암호화를 처리하기 때문에 보안이 아주 뛰어나다는 장점이 있다 그러나 IPSec은 키 관리 프로토콜인 ISAKMP/IKE의 소스 코드양이 너무 크고 복잡하여 제한된 환경에서는 구현이 어렵다는 문제점이 있지만 보안 인프라가 제대로 갖추어지면 구현의 방해 요소는 없어질 것이다 따라서 향후 보다 완벽한 암호화를 이루기 위해서는 제어연결 메시지가 암호화되어 있고 인증기능이 있는 VPN기능 중 L2TP와 IPSec을 이용하여 보안 기능이 강화된 인터넷 전화기를 구현하고자 한다

참고 문헌

[1] ITU-T Recommendation G.109, Definition of

categories of Speech Transmission Quality, September 1999

- [2] James F. Kurose and Keith W. Ross, Computer Networking-A Top-Down Approach Featuring the Internet, Addison Wesley Longman, pp.56-58-2001
- [3] K.Hamzeh, G.Pall W.Verthein, J.Taarud, W.Little,G.Zorn, "Point-to-Point Tunneling Protocol(PPTP)", RFC2637,July 1999.
- [4] TIA/EIA/TSB116, Voive Quality Recommendations for IP Telephony, March2001
- [5] ITU-T Recommendation G.114, One-Way Transmission Time, February 1996.
- [6] TIA/EIA/TSB116, Voice Quality Recommendations for IP Telephony, March 2001.
- [7] ITU-T Recommendation G.114, One-Way Transmission Time, February 1996.
- [8] A. Percy, Understanding Latency in IP Telephony, Brooktroot Technology, 1999.
- [9] VPN을 적용한 인터넷 전화 단말기의 설계에 관한연구 한국통신학회 05-30-2A-2 pp.12-20

이 성 기 (Seong gi Lee) 정회원



1982년 2월 한국항공대학교 항공통신공학과 졸업
 1985년~2003년10월 현대자동차 제품개발연구소
 2003년 전북대학교 대학원 컴퓨터공학과 박사 수료
 2004년 1월 (주) 지피텍 대표이사

<관심분야> 인공지능, 영상처리, 지능제어

유 승 선 (Seung Sun Yoo) 정회원



1988년 2월 한남대학교 전자계산학과(학사)
 1994년 2월 동대학원 전자계산공학과(석사)
 1988년 4월~2001년 6 한국에너지기술연구원 연구원
 2001년 6월 비맥(주) 기술이사
 2003년 8월 전북대학교 대학원 영상공학 박사
 <관심분야> 인공지능, 영상처리, 인터넷 통신

이 명 재 (Myung jae Lee) 정회원



1990년 3월~1999년 2월 전북대학교 전자공학과 졸업
 2002년 3월~2004년 아주대학교 대학원 E-Business MBA 졸업
 2004년 3월 전북대학교 공과대학원 영상공학과 박사과정
 1990년 3년~현재 ICC(주) 대표

이사

<관심분야> 인공지능, 영상처리, VoIP, 데이터통신

곽 훈 성 (Hoon-Sung Kwak) 정회원

한국통신학회 논문 02-27-5A-10 참조